Department of Justice
Self-Inspection Checklist for National Security Information

A. Original Classification (Section A applies only to components with Original Classification Authority (OCA))	**Yes**	**No**	**N/A**
1. Do OCAs understand the process and requirements for original classification to include: • Applicable standards and categories for classification. • Levels of classification and damage criteria associated with each one. • Avoidance of over-classification. • Classification prohibitions and limitations. • Required markings, including those for disseminating and handling. • Obsolete/invalid markings. • Determination of declassification instructions. • Delegations of OCA responsibilities. • Classification challenges.	X		
2. Have requests for Original Classification Authority been limited to those positions that have a demonstrable and continuing need to exercise this authority?	X		
3. Have OCAs prepared, as appropriate, classification guides to facilitate the proper and uniform derivative classification of information?	X		
4. Do classification guides meet the requirements of section 2.2 of the Order and § 2001.15 of the Directive?	X		
5. Have initial and updated classification guides been submitted to the DSO for written approval?	X		
6. Do all classification guides contain the minimum required information?	X		
7. Have classification guides been reviewed and updated as circumstances require, or in any event, at least once every five years?	X		
8. Does your component maintain a record of all original classification actions?	X		

B. Derivative Classification	**Yes**	**No**	**N/A**
9. Do persons who apply derivative classification markings understand the process and requirements for derivative classification, to include: • Identity of derivative classifier. • Use of source documents, including classification guides. • Declassification instructions. • Proper application of markings. • Portion marking and overall classification marking. • Classification authority block – are derivative classifiers properly identified? • Obsolete/invalid markings on source documents. • Multiple sources. • Classification challenges.	X		
10. Do persons who apply derivative classification markings observe original classification decisions and carry classification markings forward to any newly created documents?	X		

Department of Justice
Self-Inspection Checklist for National Security Information

C. Document Review	Yes	No	N/A
11. Regular reviews of representative samples of the component's original and derivative classification actions shall be conducted in accordance with § 2001.60(c)(2) of the Directive and should evaluate the classification and marking of the documents. Among the issues to consider are: • Have the standards for classification been met? • Could damage to the national security be reasonably expected in the event of unauthorized disclosure? • Have the requirements for original classification in Part 1 of the Order or for derivative classification in Part 2 of the Order been met? • Have the required markings been applied in accordance with the Order and the Subpart C of the Directive? • Have any unauthorized or invalid markings been applied to the documents?			
12. Are classified document annotated with the three separate mandatory markings (portion markings, overall classification marking, and the classification information)?	X		
13. Do originally classified documents have the proper "Classified by" line with name or personal identifier, office of origin, reason for classification and declassification instructions?	X		
14. Do derivatively classified documents have the proper "Derived From" line identifying the source and declassification instructions?	X		
15. Do derivatively classified documents include a listing of the source materials on, or attached to, each derivatively classified document?	X		
16. Are markings other than "Top Secret," "Secret," and "Confidential," (such as "FOUO", "SBU", or "Limited Official Use") used to identify classified national security information?		X	
17. Do documents that contain foreign government information (FGI) include the marking, "This Document Contains (indicate country of origin) Information?"	X		
18. Are the portions of the document that contain the FGI marked to indicate the government and classification level, using accepted country code standards, e.g., "(UK-C)?"	X		
19. If the identity of the specific government must be concealed, is the document marked, "This Document Contains Foreign Government Information," and pertinent portions shall be marked "FGI" together with the classification level, e.g., "(FGI-C)?" In such cases, is a separate record that identifies the foreign government maintained in order to facilitate subsequent declassification actions?	X		
21. Are markings uniformly and conspicuously applied to leave no doubt about the declassified status of the information and who authorized the declassification?	X		

D. Security Education	Yes	No	N/A
22. Do you maintain a classified information training program that provides for initial and refresher training and termination briefings?	X		
23. Do all personnel understand policies for classification, safeguarding, and declassification?	X		
24. Is training provided annually to all OCAs (only required if component has OCA)?	X		
25. Do all personnel who perform derivative classification receive annual training?	X		
26. Is refresher security education training conducted at least annually?	X		

Department of Justice
Self-Inspection Checklist for National Security Information

27. Are initial briefings provided in conjunction with the granting of a security clearance and prior to accessing classified information?	X		
28. Are termination briefings provided?	X		
29. Are records kept of the training that has been provided and employee participation in it?	X		
30. Are authorized couriers of classified information briefed on their responsibilities?	X		

E. Declassification	**Yes**	**No**	**N/A**
31. Is there a records management system to facilitate public release of declassified documents?	X		
32. Are procedures established for automatic, systematic, discretionary, and mandatory declassification review?	X		

F. Safeguarding	**Yes**	**No**	**N/A**
33. Is the program designed and maintained to optimize safeguarding of classified information?	X		
34. Are there control measures to prevent unauthorized access to classified information?	X		
35. Are personnel aware of procedures for identifying, reporting, and processing unauthorized disclosures of classified information?	X		
36. Are there requirements for combinations, for security and for other classified equipment?	X		
37. Are there procedures to ensure that appropriate action is taken to correct identified problems?	X		
38. Are there methods for transmitting classified information, preparing it correctly for mailing, and for hand carrying or escorting classified material?	X		
39. Do component personnel follow these requirements and procedures?	X		
40. Is classified information handled, stored, and transmitted in a way that prevents the possibility of loss or compromise?	X		
41. Is classified information restricted from disclosure to third party organizations unless there is permission from the originating component or agency?	X		
42. Do you have a system of control measures which assures that access to classified information is limited to authorized persons as well as deter and detect access by unauthorized persons?	X		
43. Is reproduction of classified information held to the minimum consistent with operational requirements?	X		
44. Is reproduction shall be accomplished only by authorized persons knowledge-able of the procedures for classified reproduction?	X		
45. Is reproduction of classified information accomplished only with approved equipment?	X		
46. Are appropriate procedures for the reproduction of classified information posted on or near equipment approved for such reproduction?	X		
47. Is classified information destroyed only by methods approved by the Security Program Operating Manual?	X		

48. Is classified material stored only in General Services Administration (GSA) approved security containers or DSO-approved open storage areas?	X		
49. Is Top Secret information stored in a GSA approved security container along with proper supplemental controls?	X		
50. Are combination safeguarded the same as the highest level of classified information that is protected by the lock? Combinations to dial-type locks shall be changed only by persons authorized access to the highest level of information stored in the container.	X		
51. Are combinations changed only by persons authorized access to the highest level of information stored in the container?	X		
52. If you have key operated locks for the storage of Secret and Confidential information has it been approved by the DSO?			X
53. Whenever key operated locks are used, have administrative procedures for the control and accounting of keys and locks been established?			X
54. Is all classified information physically transmitted outside the facility enclosed in two opaque layers; both of which provide reasonable evidence of tampering and which conceal the contents?	X		
55. Is authorization to hand-carry classified information between DOJ components and other organizations only given to DOJ personnel who have been appropriately briefed and have been specifically authorized in writing by the SPM?	X		
56. Have employees authorized to be couriers been briefed on their responsibilities, signed an acknowledgment form stating that they have received the briefing and understand their responsibilities?	X		
57. Is classified information kept under constant surveillance and covered to prevent unauthorized access when removed from storage for working purposes?	X		
58. Is a system of security checks or inspection implemented at the close of each working day to ensure that classified information is properly secured?	X		
59. Does the official responsible for arranging a conference or meeting institute procedures and select facilities which provide adequate security if classified information is to be discussed?	X		
60. Are meetings at which classified information is to be discussed held only in a U.S. Government facility or at a cleared facility of a DOJ contractor or consultant?		X	
61. Does the official responsible for hosting the meeting or conference notify each attendee of security limitations that must be imposed because of the level of access authorizations of the attendees or physical security conditions of the facility?	X		

G. Telecommunications, Automated Information Systems, and Network Security	**Yes**	**No**	**N/A**
62. Consistent with section 4.1(1) of the Order and § 2001.50 of the Directive, have uniform procedures been established to ensure that automated information systems that collect, create, communicate, compute, disseminate, process or store classified information are protected in accordance with applicable national policy issuances?	X		

Department of Justice
Self-Inspection Checklist for National Security Information

63. Have procedures been established and implemented to: • Prevent access by unauthorized persons; • Ensure the integrity of the information; and • To the maximum extent practicable use common information technology standards, protocols, and interfaces that maximize the availability of, and access to, the information in a form and manner that facilitates its authorized use; and standardized electronic formats to maximize the accessibility of information to persons who meet the criteria set forth in section 4.1(a) of the Order?	X		
64. Have all IT systems that process, store or handle classified information been certified and accredited in accordance with the requirements stated in Chapter 8 of the SPOM and guidance provided by the Department CIO?	X		
65. Do all IT hardware, firmware, and software components or products (used to for NSI) incorporated into DO J IT systems comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy Number 11?	X		
66. Are Classification Markings (Labels) that display the highest classification level and most restrictive classification category on all components of an IT system that have the potential for retaining classified information?	X		
67. Is an appropriate sensitivity and classification review performed on human-readable output before the output is released outside the security boundary to determine whether it is accurately marked with the appropriate classification and applicable associated security markings?			
68. Is media accountability implemented that provides a set of protection mechanisms comparable to those required for equivalent paper documents?			
69. Is your Classified information ONLY processed at U.S. Government facilities or approved U.S. Government contractor facilities?	X		
70. Do employees and non-DOJ personnel, including contractors, have the proper access authorizations commensurate with the highest level of information processed by the systems they access?	X		
71. Have all classified IT system users received the training specified in Chapter 3 of the SPOM and in accordance with Department CIO developed policies and standards?	X		
72. Have all IT security incidents, including virus infections, been reported to the DOJ Computer Emergency Response Team (DOJCERT)?	X		
73. If an uncleared or lower-cleared person is used for maintenance, does an appropriately cleared and technically qualified escort monitor and record the maintenance person's activities in a maintenance log?	X		
74. Is all data introduced on a classified IT system the same or lower security classification level for which the IT system is approved to operate?	X		

H. Security Violations	**Yes**	**No**	**N/A**
75. Are there procedures to conduct an inquiry/investigation of a loss, possible compromise, or unauthorized disclosure of classified information?	X		
76. Are appropriate and prompt corrective actions taken when a violation or infraction occurs?	X		
77. Are individuals who commit violations or infractions subject to appropriate sanctions?	X		

Department of Justice
Self-Inspection Checklist for National Security Information

I. Management and Oversight	Yes	No	N/A
78. Are sufficient resources and personnel committed to implement the classified national security program?		X	
79. Do security personnel fulfill their responsibilities to implement the program?	X		
80. Do the performance contracts or other rating systems include the designation and management of classified information as a critical element to be evaluated in the rating of OCAs, security managers, security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information?		X	

FBI Self-Inspection Program.

The FBI has established a Security Self-Inspection Audit program. The purpose of the self audit is to evaluate the security programs managed by a Chief Security Officer (CSO) within each FBI Field Office (FO). The Self-Inspection Audit assesses compliance within each FBI FO Security Program and covers the following areas: Security Program Management (OPSEC, Security Training, Security Incidents, and Mission Assurance), Personnel Security (initial and ongoing clearance actions), Physical Security / Access Control Processes, and Information Security (Information Assurance / Certification / Accreditation.

The Security Self-Inspection Audit is held on a bi-annual basis meaning that each FO is audited every other year. The findings and mitigation plans are coordinated through the Security Compliance Unit (SCU) and the Security Programs Unit (SPU). Once the audits are complete, the results are analyzed in order to indentify systematic program deficiencies. Those with the highest deficiencies are required to provide a "plan of action" to correct/mitigate the problem(s). At the end of the audit cycle, the FBI Inspection Division will conduct onsite reviews to verify issues identified during the self-inspection were properly addressed.

In conjunction with the Security Self-Inspection Audit, SecD established (FY12) an FBI policy creating the FBI Information Security Oversight Program (ISOP). The program will have a dedicated Program Manager who will efficiently manage the FBI's ISOP, ensuring FBI sensitive and classified information is designated, marked, handled, and declassified/de-controlled in accordance with Federal and Department of Justice (DOJ) polices.

The ISOP will assess the National Security Information (NSI), Restricted Data/Formally Restricted Data (RD/FRD), Federal Taxpayer Information (FTI), and Controlled Unclassified Information (CUI) programs to ensure they comply with Federal- Level guidelines and their implementing directives, including Executive Order 13526, Classified National Security Information.

The most recent Security Self-Inspection Audits did not reveal any deficiencies directly related to NSI.

There are no specific questions on the Security-Self Inspection Audit regarding security violations. Violations are addressed under the Security Incident Program (Security Compliance

Unit) which manages the investigations/inquiry into incidents which could involve the loss or possible compromise, or unauthorized disclosure of classified information. Security violations are reported through the Security Incident Reporting System (SIRS) and are addressed accordingly. All mitigation plans are managed by the Security Compliance Unit.

During the most recent audit cycle, there were a numbers of best practices suggested including:

(1) Leveraging automation or other information technology resources to increase efficiency and improve standardization.
(2) To insure the integrity of the audit, the use of two auditors for every self-audit regardless of the Division size is recommended.
(3) Increase frequency of collaboration between audit stakeholders.
(4) To perform consistent quality control reviews and risk analysis, establish formal, standardized operating procedures and materials for follow-up and analysis.

There are no specific questions on the Security-Self Inspection Audit regarding security violations. Violations are addressed under the Security Incident Program (Security Compliance Unit) which manages the investigations/inquiry into incidents which could involve the loss, possible compromise, or unauthorized disclosure of classified information. Security violations are reported through the Security Incident Reporting System (SIRS) and are addressed accordingly. All mitigation plans are managed by the Security Compliance Unit.

During FY11 the FBI trained over 3,000 employees on the classification and handling of NSI. These included Joint-Task Force Officers (JTTF), FBI New Agents classes, New Intelligence Analyst classes and those employees that have Original Classification Authority (OCA). For FY12, the FBI will implement a web-based training program that will include NSI classification management and the proper handling of other sensitive or controlled information.